Cover Sheet

Video Surveillance Policy

[PO.ICTF.005-01]

	Name	Signature	Date
Prepared by:	N. Fikatas		
Reviewed by:	L. Burello		
Endorsed by :	C. Manolopoulos		
Adopted by:	M. Kjaerum		

Document Control Sheet

Owner:	Head of Administration – C. Manolopoulos

Table of Contents :

Reference	Title	Pages (from-to)

Table of Contents

Log of issues:			
Issue #	Issue date	Change description	Related documents affected by new issue
01		Creation	

1 Introduction

The present policy defines the purpose and main aspects of the video surveillance equipment (referred hereafter as CCTV) installed at the premises of the Agency.

Following a building security assessment that was performed by the security services of the European Commission, it was recommended to install a video surveillance system to protect the Agency from unauthorised entry and to be able to provide evidence in case such incidents are causing potential damages.

2 Purpose and scope

For safety and security of its building, asset and visitors our Agency operates a video-surveillance system (hereafter referred as VS). This policy, along with its annexes (restricted access) describes the Agency's system and the safeguards that the Agency takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on camera.

3 Design of the system to respect privacy

3.1 Revision of the existing system

A VS was in place before the issuance of the corresponding guidelines by EDPS published on March 2010. Following the issue of the guidelines the Agency undertook and external assessment to revise its VS system and use.

3.2 Compliance status

The Agency processes the images in accordance with both the Guidelines and Regulation (EC) No 45/2001 on the protection of personal data by the Community institutions and bodies.

3.3 Notification of compliance status to the EDPS

The Agency consulted EDPS when defining the present policy.

Certain text is restricted from public version

3.4 Contacts with the relevant data protection authority in the Member State.

The competent data protection authority in Austria was informed in July 2011. Proactively, the Agency installed the on-the-spot notices in German to inform pedestrians and visitors.

3.5 Director's decision and consultation

(Restricted from public version)

3.6 Transparency

The Video-surveillance Policy has two versions, a version for restricted use and this public version available and posted on our internet (http://fra.europa.eu/fraWebsite/about_fra/who_we_are/data_protection/data_protection_en.htm) and intranet site (http://intrafra/ADMINISTRATION/QUALITYMANAGEMENT/Pages/Policies%20and%20Standard.aspx)

The public version of the Video-surveillance Policy may contain summary information with respect to particular topics or attachments. When this is the case, it is always clearly stated. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling reasons (e.g. for security reasons or to preserve the confidentiality of commercially sensitive information or to protect the privacy of individuals).

3.7 Periodic reviews

A periodic data protection review will be undertaken by the security office with the presence of the DPO every two years, the first by 30 December 2012. Where feasible, the Agency may invite a DPO from another EU institution to undertake the review.
During the periodic reviews we will re-assess :

- The need for the video-surveillance system,
- that the system continues to serve its declared purpose, and that
- that adequate alternatives remain unavailable.

(Restricted text)

3.8 Privacy-friendly technological solutions

Following the revision of the initial VS, the Agency implemented the following privacy-friendly technological solutions:

- Masking or scrambling images to help eliminate surveillance of areas irrelevant to our surveillance target. This technique is also useful to edit out images of third persons when providing access to the images of a data subject. See also its use to protect facial images or number plate information when operating a webcam.
- Restricted access to systems and data
    - Physical access to the area where the recordings are stored is only possible by the Security guards and the Facilities Office staff that are responsible for the building management.
    - All access to the recording system requires the use of username and password and different access rights are provided to Facilities and Security staff
    - The location of the monitors is such that no unauthorised person can have access to them or possibility to view the footage

- Recording system employs an overwrite technology thus ensuring any previous data pass the retention period is erased. Therefore there is no need for the disposal of storage media.

4 Surveillance areas

(Restricted text)

5 Collection of personal information

(Restricted text)

6 Purpose of the surveillance

The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to our building and helps ensure the security of our building, the safety of our staff and visitors, as well as property and information located or stored on the premises.
It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support our broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault).

6.1 Purpose limitation

The system is not used for any other purpose, for example, it is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigating physical security incidents such as thefts or unauthorised access) It is only in exceptional circumstances that the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation as described in Section 8

1. The Agency foresees no ad hoc surveillance for which it needs to plan at this time
2. Webcams. The Agency has no webcams used for surveillance
3. No special categories of data collected.

7 What is the lawful ground and legal basis of the video-surveillance?

The use of our video-surveillance system is necessary for the management and functioning of our Agency for the security and access control purpose described above). Therefore, the Agency has a lawful ground for the video-surveillance A more detailed and specific legal basis for the video-surveillance is provided in this Video-surveillance Policy. This policy, in turn, forms part of the broader security policies adopted by the Agency.

8 Access to data and disclosures

Access to data: In-house security staff and outsourced security-guards. Recorded video is accessible to the above but there are different access rights assigned to them. The Facilities office has full access to the footage. Live video is also accessible to security guards on duty. These security guards work for an outsourced security company.

Furthermore, the following have been put in place:

- Physical access to the area where the recordings are stored is only possible by the Security guards and the Facilities Office staff that are responsible for the building management including security aspects.
- All access to the recording system requires the use of username and password and different access rights are provided for each user.
- Responsible staff(security guards and Facilities office staff) have access as follows:
    1. view the footage real-time,
    2. view the recorded footage,
    3. download and copy footage
    4. Delete and alter footage (only Facilities office has access)

- The location of the monitors is such that no unauthorised person can have access to them or possibility to view the footage
- Recording system employs an overwrite technology thus ensuring any previous data pass the retention period is erased. Therefore there is no need for the disposal of storage media.

Retention period: The retention period of the footage is currently 4 days and then the footage is overwritten.

Access rights: Data can be accessed by the Head of Administration, the Facilities Office staff members of the Agency and the contracted security company as bounded by the contractual arrangements between the two parties. Only the Facilities Office staff of the Agency will be granted access to the data via password and the password. No data will be transferred to external parties.

Data Subjects are informed of the following rights in line with Article 13, 14, 15, 16, 17, 18 of Regulation 45/2001:

- Right to access data – in order to exercise this right, Data Subjects have to:
    1. Send a request to the Head of Administration, who will assess if the reason is legitimate in accordance to the Staff Regulations, Regulation 45/2001 and other related regulations and no restrictions apply.
        a. Once the reason is proved valid, the Head of Administration will pass the request to the security staff member.
        b. In case the reason is not proved valid, a response to the data subject will be given mentioning why access cannot be provided.
    2. A response mentioning whether the access request is valid or not should be provided within 10 working days upon official receipt of the request.
    3. The security staff member must ensure before providing access to the staff member, that information including only the staff member in question is accessible for view. If another data subject is included then access to such footage will not provided before receiving the consent of the involved staff member. Access to information will be provided within 5 working days upon approval of the request. No fee will be charged.

- Right to block – The data subjects can request from the Data Controller the blocking of their personal data. Blocking is not possible in case of an official investigation.
- Right to rectify – Rectification of CCTV footage is not allowed. However, the data subject can exercise his right of rectification on the report written by security staff in connection with a security incident.

- Right to object – This right is not applicable due to the Legal basis under which the data are processed.

- Right to erase data – Data subjects have the right to obtain from the Data Controller the erasure of data if their processing is unlawful.

- Right to have recourse at any time to the European Data Protection Supervisor (EDPS).

Data protection training: The outsourced security guards, were given their first data protection training when they started working at the Agency. Training on Data Protection is provided on an annual basis including newcomers.

Confidentiality undertakings: After the training of involved persons a confidentiality undertaking is signed. This undertaking was also signed by the outsourced company.

Transfers and disclosures: All transfers and disclosures outside the facilities office are documented and subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing.
The DPO of the Agency is consulted in each case.

No access is given to management or human resources.

Local Authorities may be given access if needed to investigate or prosecute criminal offences. This is done upon a written request by the Authorities. In case there is an investigation of the Authorities, it is obliged to obtain a "waiver of immunity" if footage concerns an EU staff member.

In such cases, the incident is logged in the log form incident indicating the purpose. The Agency ensures that only footage related to the specific incident is disclosed to the Authorities.

Under exceptional circumstances, access may also be given to:

- the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF,
- the Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or
- those carrying out a formal internal investigation or disciplinary procedure within the Institution

provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence.

No requests for data mining are accommodated.

9 How do we protect and safeguard the information?

In order to protect the security of the video-surveillance system, including personal data, a number of technical and organisational measures have been put in place. (Restricted text)

10 How long do we keep the data?

The images are retained for a maximum of 96 hours. Thereafter, all images are overwritten by the system with newer footage. If any image needs to be stored to further investigate or evidence a security incident, they may be retained as necessary. Their retention is rigorously documented and the need for retention is periodically reviewed.

11 How do we provide information to the public?

Multi-layer approach: We provide information to the public about the video- surveillance in an effective and comprehensive manner. To this end, we follow a multi-layer approach, which consists of a combination of the following two methods:

- on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing, and
- we post this Video-surveillance Policy on our intranet and also on our internet sites for those wishing to know more about the video-surveillance practices of the Agency
- Print-outs of this Video-surveillance Policy are also available at our building reception desk and from our Facilities Office upon request. A phone number and an email address are provided for further enquiries.

We also provide on-the-spot notice adjacent to the areas monitored. We placed a notice near the main entrance, indicative signs in the local language with an image are installed outside the building and the information note for data subjects is available in the entrance area.

Specific individual notice: In addition, individuals will be given individual notice if they were identified on camera (for example, by security staff in a security investigation) provided that one or more of the following conditions also apply:

- their identity is noted in any files/records,
- the video recording is used against the individual,
- kept beyond the regular retention period,
- transferred outside the security unit, or
- if the identity of the individual is disclosed to anyone outside the security unit.

(Restricted test)

12 How can members of the public verify, modify or delete their information?

Members of the public have the right to access the personal data we hold on them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing of personal data should be directed to Mr Manolopoulos, Head of Administration constantinos.manolopoulos@fra.europa.eu. He or she may also be contacted in case of any other questions relating to the processing of personal data.

Whenever possible, the facilities office responds to an enquiry in substance within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reason for the delay within 15 days. Even in the most complex of cases access must be granted or a final reasoned response will be provided rejecting the request within three months at the latest. The Facilities Office will do its best to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images on a DVD or other media. In case of such a request, the applicants must indicate their identity beyond doubt (e.g. they should bring identity cards when attending the viewing) and, whenever possible, also designate the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph of themselves that allows the responsible staff to identify them from the images reviewed.

At this time, we do not charge applicants for requesting a viewing or a copy of their recorded images. However, we reserve the right to charge a reasonable amount in case the number of such access requests increases.

An access request may be refused when an exemption under Article 20(1) of Regulation 45/2001 applies in a specific case. For example, following a case-by-case evaluation we may have to conclude that restricting access may be necessary to safeguard the investigation of a criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also present on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to use image-editing to remedy the lack of consent.

13 Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under Regulation 45/2001 have been

infringed as a result of the processing of their personal data by the Agency. Before doing so, we recommend that individuals first try to obtain recourse by contacting:

- the Head of Administration
- the data protection officer of the Agency email: dpo@fra.europa.eu

Staff members may also request a review from their appointing authority under Article 90 of the Staff Regulation.